

Web-Security - Mediawiki

Hardening Mediawiki

Planning and implementing
a Security architecture

Intrusion Detection and Prevention
System based on PHPIDS

Web-Security - Mediawiki

Team:

- Patrick Schneider
- Eric Hartmann
- Björn Rathjens
- Thomas Kraebihl
- Contact: patrick.schneider@mni.fh-giessen.de
- Tobias Homberg
- Mark Schlüter
- Christopher Allan

Web-Security - Mediawiki

Demo system:

- <https://hardening-mediawiki/index.php>
(host "212.201.8.11 hardening-mediawiki" has to be set)
- htaccess: HMW / WebSec2010

Web-Security - Mediawiki

Source code:

- Trac bugtracking system:
 - https://trac.mni.fh-giessen.de/trac/HMW_SS10
- SVN access available at:
 - https://svn.mni.fh-giessen.de/repositories/HMW_SS10/trunk/

Documentation:

- https://wiki.mni.fh-giessen-friedberg.de/index.php/WebSecurity_-_Mediawiki
- <http://www.mediawiki.org/wiki/Extension:PhpIds>

Web-Security - Mediawiki

Administration

- Configuration via the PHPIDS Manager
 - IDS/IPS status
 - PHPIDS parameters
 - Log/warn/ban thresholds
 - Rules
- Statistics
 - Impact log
 - Attackers
- Server security settings

PHPIDS Administration

MediaWiki.Care
"Where your Wiki is safe"

PHPIDS Manager

Verwaltung Rules Impactlogs Stats Systemsicherheit

Benutzer sperren | gesperrte Benutzer 1 | installierte Erweiterungen

Verwaltung

Status ☒ on ☐ off

IPS-Status ☒ on ☐ off

Artikelfelder überwachen ☐ on ☒ off

Filtertyp

Basispfad

Empfänger

Filterpfad

tmp pfad

Keys prüfen? ☒ false ☐ true

Logging Path

eMail-Betreff

zusätzliche Mail-Header

Wrapper

Loglimit

Logsite

Warnlimit

Warnsite

Logoutlimit

Logoutsite

Banlimit

Bansite

Ausnahmen

Tags (Statistik)

Die Werte werden durch „geteilt“

Web-Security - Mediawiki

PHPIDS Rules

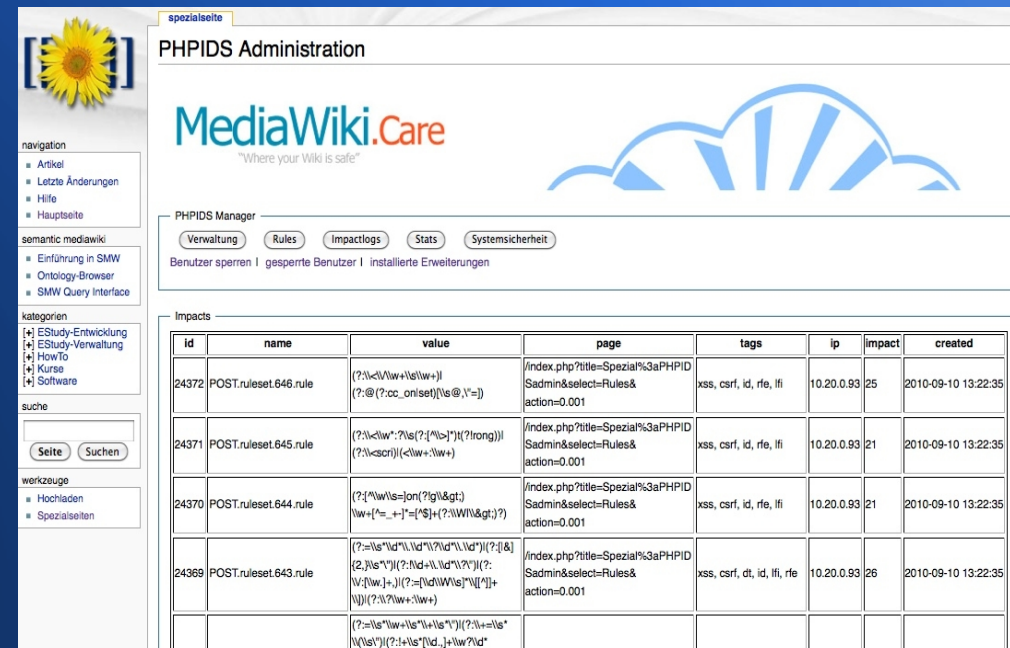
- List of active Rules
 - Name
 - Description
 - Attack type
 - Impact value
 - Tag „autogenerated rule“
- Import rulesets via XML file
- Manually add / edit / delete rules

[illegible]

Web-Security - Mediawiki

Impactlogs

- Attack vector
 - Affected variable
 - Suspicious value
 - Attacked page
- Impact value
- IP Address of attacker
- Time of attack



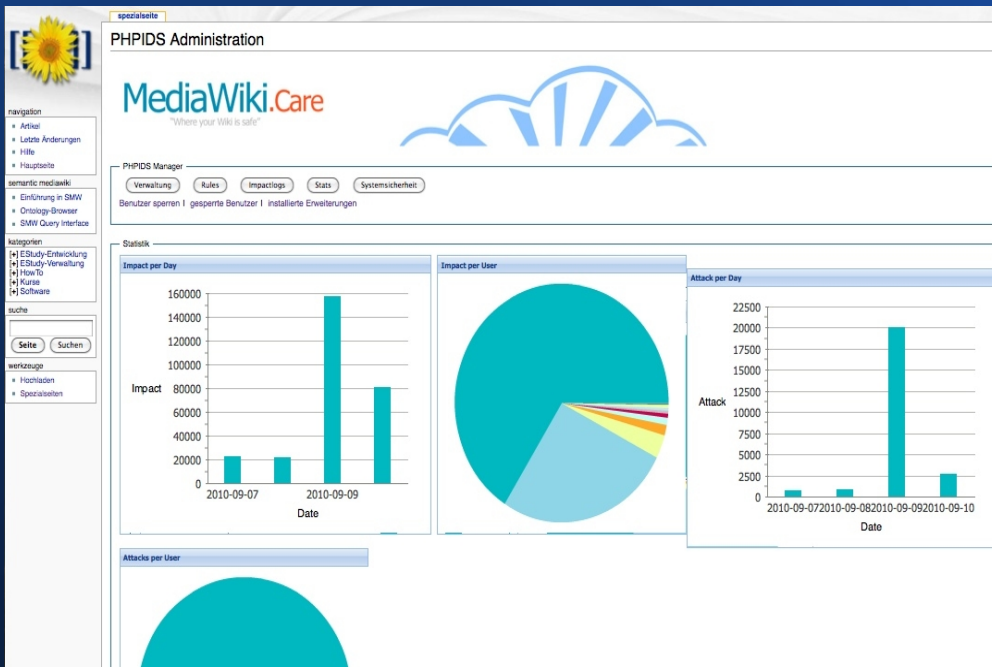
The screenshot shows the MediaWiki.Care PHPIDS Administration interface. The top navigation bar includes a sun icon and the text "spezielleite". The main header features the "MediaWiki.Care" logo with the tagline "Where your Wiki is safe". Below the header, there's a "PHPIDS Manager" section with tabs for "Verwaltung", "Rules", "Impactlogs", "Stats", and "Systemicherheit". The "Impactlogs" tab is active, displaying a table of attack logs. The table has columns for "id", "name", "value", "page", "tags", "ip", "impact", and "created". The table contains five rows of data, each representing a different attack event.

id	name	value	page	tags	ip	impact	created
24372	POST.ruleset.646.rule	(?<[\\w+\\W+]) (?<[\\w+\\W+])	/index.php?title=Spezial%3aPHPID Admin&select=Rules& action=0.001	xss, csrf, id, rfe, ifi	10.20.0.93	25	2010-09-10 13:22:35
24371	POST.ruleset.645.rule	(?<[\\w+\\W+]) (?<[\\w+\\W+])	/index.php?title=Spezial%3aPHPID Admin&select=Rules& action=0.001	xss, csrf, id, rfe, ifi	10.20.0.93	21	2010-09-10 13:22:35
24370	POST.ruleset.644.rule	(?<[\\w+\\W+]) (?<[\\w+\\W+])	/index.php?title=Spezial%3aPHPID Admin&select=Rules& action=0.001	xss, csrf, id, rfe, ifi	10.20.0.93	21	2010-09-10 13:22:35
24369	POST.ruleset.643.rule	(?<[\\w+\\W+]) (?<[\\w+\\W+])	/index.php?title=Spezial%3aPHPID Admin&select=Rules& action=0.001	xss, csrf, id, rfe, ifi	10.20.0.93	26	2010-09-10 13:22:35
		(?<[\\w+\\W+]) (?<[\\w+\\W+])					

Web-Security - Mediawiki

Statistics

- Graphical visualization
 - based on ExtJS
 - Timeframe configurable
- Impacts per day (sum, bar graph)
- Attacks per day (sum, bar graph)
- Impacts per user (piechart)
- Attacks per user (piechart)



Web-Security - Mediawiki

System security

- Versions of installed packages
 - PHP version
 - Suhosin version
 - MySQL client version
 - MySQLi client version
 - PHPIDS version
 - Mediawiki version
 - PHPIDS Admin version
- Suhosin parameters



Paket	Version	Projektseite
PHP-Version	5.2.6-1+lenny9	http://www.php.net
Suhosin-Version	0.9.27	http://www.hardenod-php.net/suhosin
MySQL-Client-Version	5.0.51a	
MySQLi-Client-Version	5.0.51a	
PHP-IDS-Version	0.6.4	http://php-ids.org
Mediawiki-Version	1.15.1 (1763)	http://www.mediawiki.org
PHPIDS Admin-Version	0.1	https://trac.mni.fh-giessen.de/

Suhosin Einstellungen	
suhosin.apc_bug_workaround	0
suhosin.cookie.checkraddr	0
suhosin.cookie.cryptdocroot	1
suhosin.cookie.cryptkey	[protected]
suhosin.cookie.cryptlist	
suhosin.cookie.cryptraddr	0
suhosin.cookie.cryptua	1

Web-Security - Mediawiki

OWASP - Top 10 Application Security Risks –2010

- A1 : SQL-Injection
 - Prevented by MediaWiki database abstraction layer
 - Scan has shown no vulnerable script
- A2 : Cross-Site Scripting (XSS)
 - Prevented by MediaWiki input validation
- A3 : Broken Authentication and Session Management
 - Session Management secured by https and suhosin
 - Secure authentication provided by CAS

Web-Security - Mediawiki

OWASP - Top 10 Application Security Risks –2010

- A4 : Insecure Direct Object References
 - Prevented by MediaWikis security tokens
 - Low risk scenario in MediaWiki
- A5 : Cross-Site Request Forgery (CSRF)
 - Prevented by MediaWikis security token
- A6 : Security Misconfiguration
 - Show security settings and software versions

Web-Security - Mediawiki

OWASP - Top 10 Application Security Risks –2010

- A7 : Insecure Cryptographic Storage
 - Secured by CAS and suhosin
- A8 : Failure to Restrict URL Access
 - No private pages, directories secured by htaccess
- A9 : Insufficient Transport Layer Protection
 - Always using https, cookies encrypted by suhosin
- A10: Unvalidated Redirects and Forwards
 - Possibly vulnerable (links are allowed, low risk scenario)

Web-Security - Mediawiki

Thanks for your attention!